CLAIMS

What is claimed is:

1. A method for caching secure network communications in a computer network, comprising placing at least one secure reverse proxy among at least one web server and at least one web browser, wherein the at least one secure reverse proxy caches secure content.

2. A method for secure network communications, comprising:

coupling at least one network appliance among at least one web server and at least one web browser;

establishing a secure session between the at least one network appliance and the at least one web browser, wherein the at least one web browser sends an encrypted request for content using a secure session protocol;

decrypting the encrypted request for content at the at least one network appliance;

examining at least one network appliance's local cache to locate the content;

encrypting the content from the at the at least one network appliance's local cache using an established secure protocol; and

sending the content to the at least one web browser, wherein reducing the number of requests at the web server for establishing a secure network connection improves network efficiency.

3. The method of claim 2, wherein the local cache includes non-volatile memory.

4. The method of claim 2, wherein the at least one network appliance and the at least one Web server are collocated.

5. The method of claim 2, wherein the content includes an HTTP page.

6. The method of claim 2, wherein decrypting further includes:

determining the content requested by the at least one web browser is not present in the at least one network appliance's local cache;

forwarding the request for content to the at least one web server using a separate secure session;

receiving back from the at least one web server to the at least one network appliance a response containing the requested content, wherein communication between the at least one network appliance and the at least one web server is secure; and

caching the requested content locally at the network appliance for future requests.

7. The method of claim 2, wherein the secure session uses Transport Layer Security protocol.

8. The method of claim 2, wherein the secure session uses Secure Socket Layer protocol.

9. The method of claim 2, wherein the secure session uses Internet Protocol Secure ("IPSec") techniques.

10. A method for caching secure network communications, comprising:

coupling at least one Secure Reverse Proxy ("SRP") among at least one web server and at least on web browser wherein the at least one SRP intercepts requests from the at least one web browser to establish a secure network communication session with the at least one web server;

establishing a first secure session using a first secure session protocol between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an encrypted request for a HTTP page;

decrypting the encrypted request for a HTTP page at the at least one SRP using the first secure session protocol, wherein the at least one SRP examines a local cache determining if the HTTP page is available;

retrieving the HTTP page if available from the local cache;

encrypting the HTTP page retrieved from the local cache using the first secure session protocol;

sending the encrypted HTTP page to the at least one web browser if the HTTP page is available from the local cache using the first secure session;

establishing a second secure session using a second secure session protocol with the at least on web server if the HTTP page is not available from the local

cache, wherein the second secure session is maintained;

encrypting the request for a HTTP page using the second secure session protocol;

forwarding the request for a HTTP page encrypted using the second secure session to the at least one web server:

receiving from the at least one web server an encrypted HTTP page using the second secure session;

decrypting the encrypted HTTP page using the second secure session protocol;

storing the HTTP page in the at least one SRP's local cache;

encrypting the HTTP page using the first secure session protocol; and

sending the HTTP page to the at least one web browser using the first secure session.

11. The method of claim 10, wherein coupling includes connecting the SRP and web server using a dedicated line.

12. The method of claim 10, wherein coupling includes having the web server and SRP collocated.

13. The method of claim 10, wherein storing includes using non-volatile media to store the content.

14. The method of claim 10, wherein storing includes encrypting the content using a third secure session protocol.

15. The method of claim 10, wherein the first secure session protocol includes Transport Layer Security protocol.

16. The method of claim 10, wherein the second secure session protocol includes Transport Layer Security protocol.

17. The method of claim 10, wherein the third secure session protocol includes Transport Layer Security protocol

18. The method of claim 10, wherein the first secure session protocol includes Secure Socket Layer protocol.

19. The method of claim 10, wherein the second secure session protocol includes Secure Socket Layer protocol.

20. The method of claim 10, wherein the third secure session protocol includes Secure Socket Layer protocol

21. The method of claim 10, wherein the first secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

22. The method of claim 10, wherein the second secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

23. The method of claim 10, wherein the third secure session protocol includes Internet Protocol Secure ("IPSec") techniques.

24. A method for caching secure content in a Secure Reverse Proxy ("SRP") in an secure network, comprising:

coupling at least one SRP among at least one web browser and at least one web server wherein the at least one SRP receives from the at least one web browser requests for establishing a first secure session;

establishing the first secure session using a first secure session protocol between the at least one SRP and the at least on web browser, wherein the web browser sends an encrypted request for content to the at least one SRP;

decrypting the encrypted request for content from the at least one web browser at the at least one SRP using the first secure session protocol, wherein the at least one SRP determines that the at least one SRP does not possess the requested content;

establishing a second secure session using a second secure session protocol between the at least one SRP and the at least one web server, wherein the second secure session is maintained;

encrypting the request for content from the at least one web browser using the second secure session protocol;

sending the encrypted request for content to the at least one web server using the second secure session;

receiving the content from the at least on web server at the least one SRP

using the second secure session;

decrypting the content using the second secure session protocol;

storing the requested content locally in a memory at the at least one SRP; and

retrieving the content from the memory at the at least one SRP upon subsequent requests for the content.

25. The method of claim 24, wherein storing includes encrypting the content using a third secure session protocol, wherein the third secure session protocol is known only to the at least one SRP.

26. The method of claim 24, wherein storing includes using non-volatile media.

27. The method of claim 24, wherein coupling includes establishing a dedicated secure line between the SRP and the web server.

28. The method of claim 24, wherein coupling includes collocating the web server and the SRP.

29. The method of claim 24, wherein content includes an HTTP page.

30. The method of claim 24, wherein the first secure session includes Transport Layer Security protocol.

31. The method of claim 24, wherein the second secure session includes Transport Layer Security protocol.

32. The method of claim 24, wherein the first secure session includes Secure Socket Layer protocol.

33. The method of claim 24, wherein the second secure session includes Secure Socket Layer protocol.

34. The method of claim 24, wherein the first secure session includes Internet Protocol Secure ("IPSec") techniques.

35. The method of claim 24, wherein the second secure session includes Internet Protocol Secure ("IPSec") techniques.

36. The method of claim 24, wherein storing includes encrypting the requested HTTP page.

37. A system for caching secure communications in a network comprising:

at least one web server;

at least one web browser;

at least one Secure Reverse Proxy ("SRP") coupled among the at least one

web server and the at least one web browser, wherein the at least one SRP caches secure content.

38. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Transport Layer Security protocol to establish a secure session.

39. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Secure Socket Layer protocol to establish a secure session.

40. The system of claim 37, wherein the at least one web browser, the at least one web server, and at least one SRP use Internet Protocol Secure ("IPSec") techniques to establish a secure session.

41. A method for secure communications in a network, comprising:

caching responses including secure content from at least one web server to at least one web browser in at least one Secure Reverse Proxy ("SRP"), wherein the at least one SRP is coupled among the at least one web server and the at least one web browser; and

enabling future requests for the same secure content to be processed by the at least one SRP.

42. A system for enhancing secure communications in a computer network, comprising:

at least one Secure Reverse Proxy ("SRP") coupled among at least one web server and at least one browser, wherein the at least one SRP establishes a secure session between the at least one SRP and the at least one web browser;

the at least one web browser sending to the at least one SRP an HTTP page request encrypted using the secure session protocol;

the at least one SRP decrypting the HTTP page request, wherein the SRP examines a local cache to locate the HTTP page, retrieves the HTTP page, encrypts the HTTP page from the local cache using the established secure session protocol, and sends the HTTP page to the at least one web browser using the secure session reducing the messages sent to the web server improving the efficiency of the network.

43. The system of claim 42, wherein the secure session is established using Transport Layer Security protocol.

44. The system of claim 42, wherein the secure session is established using Secure Socket Layer protocol.

45. The system of claim 42, wherein the secure session is established using Internet Protocol Secure ("IPSec") techniques.

46. The system of claim 42, further comprising:

the at least one SRP establishing a separate secure session with the at least one web server, wherein the at least on web server forwards the HTTP page request to the at least one web server using a separate secure session;

the at least one web server sending to the at least one SRP a response containing the requested HTTP page, wherein communication between the at least one SRP and the at least one web server is secure using the separate secure session; and

the at least one SRP caching the requested HTTP page for future requests.

47. A computer-readable medium, comprising executable instructions for caching secure content in computer network which, when executed in a processing system, causes the system to:

couple at least one Secure Reverse Proxy ("SRP") among at least one web server and at least one browser;

direct requests for establishing a secure connection from the at least one web browser to the at least one SRP, wherein the SRP responds by initiating an initial secure handshake;

establish a secure session between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an HTTP page request encrypted using a secure session protocol;

decrypt the HTTP page request at the at least one SRP, wherein the SRP examines a local cache to locate the HTTP page;

retrieve the HTTP page from the local cache;

encrypt the HTTP page from the local cache at the at least one SRP using the established secure protocol; and

send the HTTP page to the at least one web browser, wherein contact with the at least one web server is reduced improving the effective efficiency of the network.

48. The computer readable medium of claim 47, further comprising instructions that when executed in a processing system cause the system to:

forward the HTTP page request to the at least one web server using a separate secure session when the HTTP page is not present in the local cache;

receive from the at least one web server to the at least one SRP a response containing the requested HTTP page wherein communication between the at least one SRP and the at least one web server is secure using a separate secure session; and

cache the requested HTTP page locally at the SRP for future requests.

49. An electromagnetic medium containing executable instructions for improving secure connections in computer network communications which, when executed in a processing system, causes the system to:

couple at least one Secure Reverse Proxy ("SRP") among at least one web server and at least one browser;

direct requests for establishing a secure connection from the at least one web browser to the at least one SRP, wherein the SRP responds by initiating an initial secure handshake;

establish a secure session between the at least one SRP and the at least one web browser, wherein the at least one web browser sends an HTTP page request encrypted using a secure session protocol;

decrypt the HTTP page request at the at least one SRP, wherein the SRP examines a local cache to locate the HTTP page;

retrieve the HTTP page from the local cache;

encrypt the HTTP page from the local cache at the at least one SRP using the established secure protocol; and

send the HTTP page to the at least one web browser, wherein contact with the at least one web server is reduced improving the effective efficiency of the network.

50. The electromagnetic medium of claim 49, further comprising instruction that when executed in a processing system cause the processing system to:

forward the HTTP page request to the at least one web server using a separate secure session when the HTTP page is not present in the local cache;

receive from the at least one web server to the at least one SRP a response containing the requested HTTP page wherein communication between the at least one SRP and the at least one web server is secure using a separate secure session; and

cache the requested HTTP page locally at the SRP for future requests.